ESP - Policy

25X1 [redacted] Executive Secretary, Intelligence Community Staff, the Director of Central Intelligence memorandum to the Senior Interagency Group (Intelligence) dated April 20, 1984, classified "secret," entitled "April 27, 1984, Meeting," regards a meeting at 10:00 a.m. on April 27, 1984. The meeting will be held in the Community Headquarters Building (Room 6W02) and will be chaired by the Director of Central Intelligence; attendance will be principals plus one.

The following items will be addressed:

Hostile Intelligence Threat Assessment and Initiatives to Combat Unauthorized Disclosures of Classified Intelligence Information.

The following is a summary of TAB A, a memorandum
25X1 for General Counsel from [redacted] Associate General Counsel/Chairman, Unauthorized Disclosures Investigation Committee, SECOM, the subject of which is "Intelligence Leaks." TAB A is attached to a memorandum from Eloise R. Page, Deputy Director, Intelligence Committee Staff for Director of Central Intelligence, dated April 6, 1984, captioned "Initiatives to Combat Unauthorized Disclosures of Classified Intelligence Information."

1. Summary: Initial paragraph discusses unauthorized disclosures having become common place where leakers have turned into heroes and security officials into villains.

   Comment: No comment.

25X1 2. Summary: This paragraph refers to [redacted] looking for a more vigorous program of security awareness in which those individuals who violate their trust from Government service should be dealt with more harshly in a public and visible
25X1 manner. [redacted] additionally states that there must be a law separate from espionage statutes which criminalizes the unauthorized disclosures of classified information by Government employees.

   Comment: Review of this paragraph by the FBI shows validity and the FBI poses no objection to the thought of establishing separate laws to deal with unauthorized disclosures of classified information as opposed to the current handling under the espionage statutes.

25X1 3. Summary: Paragraph 3 expresses [redacted] opinion that although security is not an exact science, the CIA has established a model system. He explains their system requires rigorous security indoctrination from the beginning of the person's employment with that agency. Their system is based on fostering a system of values geared to protect intelligence sources and methods among their employees. Media contacts are centralized and controlled. Their employees are subjected to polygraph examinations throughout their employment. Security breechers are punished and "potential leakers know that their jobs will be forfeited."

   Comment: The CIA program, although in context has proven to be one of the best systems, has not, in itself, proven infallible.

4. Summary: This paragraph relates to the CIA's and NSA's operating under the same security controls which 25X1 alleges do not exist in consumer (receiver) agencies. 25X1 insists that the same standards by both the producer (supplier) and consumer operate on the same standards in order to reassure adequate security of classified information.

Comment: The security controls for the CIA and NSA may exist under one system and considered to be secure; however, the FBI's system, although not identical to the system of CIA and NSA, is in conformance with the guidelines as established by the Director of Central Intelligence.

5. Summary: This paragraph discusses the need to more carefully prepare communications containing intelligence information so as to protect the sources and methods utilized in acquiring this information. It also concerns the need to prudently disseminate information on a strict need-to-know basis. It discusses the greater use of the "read-and-return" programs. It also concerns implementation of search programs for persons exiting Government buildings which house classified information to preclude classified documents being carried from the buildings or being stockpiled in homes or other offices.

Comment: The FBI agrees with the information stated in this paragraph but has concerns over implementing a broad search 25X1 procedure as mentioned. examples are well stated but do not appear to be practical.

6. Summary: This brief paragraph is a basic statement suggesting that changes must be accomplished in routine business and new 25X1 approaches must be developed. As an example, mentioned not allowing press unrestricted access through Government offices.

Comment: This policy is currently in effect by the FBI to restrict access of the news media and all other individuals (non-FBI employees) who do not have a specific requirement for unrestricted access to our facilities.

7. Summary: This paragraph discusses moving to a computer-assisted dissemination system in which the security modules would provide a record as to which documents and to whom these documents were presented. This system would provide for the computer to generate a unique number for each document that is produced.

Comment: The FBI has great successes in utilizing computers with the storage of classified information in both the counterintelligence and terrorism areas; however, it would

appear that to implement a system of transmitting classified documents by computer from one agency to another would provide insurmountable obstacles that can better be served by utilization of proper manpower controls.

25X1 8. Summary: [redacted] expresses the need to focus on the use of personal microcomputers which can store classified data which can provide the flexibility of being easily transported. 25X1 [redacted] does mention that sources and methods of information should be protected against being incorporated into such personal computers.

Comment: With the utilization of personal microcomputers to store classified data, the chances of compromising this information do increase as unauthorized individuals may have access to the terminal inside or out of the Government facility.

9. Summary: This paragraph discusses the photocopying of highly classified intelligence publications and the need to curtail this practice and thus avoid having these documents "lying 25X1 around." Again, [redacted] refers to utilizing computers as well as developing a "classified executive suite" for use by senior policy customers outside the intelligence community. 25X1 [redacted] describes this "classified executive suite" as an attractively furnished room where senior officials can read classified intelligence publications by tying into a computer terminal with a personal identification key. After reviewing the publication on the computer screen, the senior official can request a hard copy which will be recorded through the computer terminal.

Comment: This type of storage for classified information could prove extremely costly in that senior officials of the Government might be required to leave their agency and travel to a second location where this "classified executive suite" has been established to review classified information. This system appears unrealistic and with the appropriate guidelines as set forth as currently practiced by the FBI, by the Director of the CIA, for storage of classified information being enhanced, there should be no need for such an ellaborate classified document review system.

25X1 10. Summary: [redacted] in this paragraph, states that intelligence leaks should be investigated in a systematic way with more attention needed for damage assessment and evaluation of the 25X1 information that has been leaked. [redacted] states that investigations conducted by various agencies are often

inadequate, and in many case, responsibility and authority for the investigation "stops at the water's edge." As a
25X1 solution, [redacted] recommends that the Department of Justice and the FBI rigorously investigate the unauthorized disclosure of classified intelligence information, especially when intelligence sources and methods are involved.

Comment: The FBI currently investigates unauthorized disclosures of classified information in an efficient and thorough manner pursuant to instructions and policy set forth by the Department of Justice. Upon completing all avenues of an unauthorized disclosure of classified information investigation, the facts as obtained through investigation are then presented to the Department of Justice for their prosecutive opinion.

25X1 11. Summary: [redacted] relates in this paragraph that very few leaks reported to the Department of Justice by the CIA are
25X1 investigated. [redacted] refers to a letter that the CIA receives from the Department of Justice which routinely states that due to the level of dissemination of the information disclosed, the Department of Justice is reluctant to direct the FBI to investigate this matter unless an individual is identified who actually is suspected of releasing the classified information.

Comment: In the course of routine business, the Department of Justice forwards to the FBI those cases that are deemed appropriate for FBI investigation, and these matters are appropriately addressed and brought to a logical conclusion. As a matter of course, the FBI has and will continue to investigate all unauthorized disclosures of classified information when directed to do so by the Department of Justice whether or not a suspect is known.

25X1 12. Summary: In this paragraph, [redacted] states "the FBI will not investigate until we identify the suspects is incredible."
25X1 [redacted] goes on to explain that this is similar to the police stating they will not investigate a bank robbery in an area like New York's Fifth Avenue because too many people were in the area; however, if the subject is identified, then the
25X1 police would respond. [redacted] then expresses some investigative techniques that he feels would be adequate in unauthorized disclosure cases; for example, he states "a simple examination of who stands to benefit from the leak can
25X1 help to focus an FBI investigation." [redacted] additionally advises that when the CIA's Office of Security provides lead information, the CIA rarely finds that the Department of Justice is interested in pursuing the matter.

25X1 Comment: It is apparent from this paragraph [redacted] is not aware of the investigative techniques utilized in FBI investigations and further, when an FBI investigation is initiated, all avenues of the investigation, to include areas of susceptibility, are identified and brought to the attention
25X1 of that respective agency. The notion that [redacted] has that the FBI will not investigate a case until the subject is fully identified is ludicrous and certainly not factual. As stated in previous comments, when the FBI has been advised of an investigation within its jurisdiction, this matter is aggressively pursued and all logical investigation is presented to the Department of Justice for a prosecutive opinion.

13. Summary: This paragraph implies that the Department of Justice regards the chances of solving a leak case as poor, and it prefers to direct FBI resources toward other investigative responsibilities, i.e. espionage matters. In summarizing
25X1 this paragraph, [redacted] states that is it fair to say "that Justice and the Bureau do not see much glory or career enhancing statistics emerging from leak investigations and they act accordingly."

Comment: As reiterated previously, the FBI accepts for investigation all referrals and seeks no glory or career enhancing opportunities in investigating those cases within the FBI's jurisdiction whether leak cases or otherwise. The FBI can only respond to those matters which are referred within jurisdictional boundaries from the Department of Justice and will continue to aggressively pursue these matters.

25X1 14. Summary: [redacted] is suggesting in this paragraph that a special unit in the FBI be created with the sole responsibility
25X1 to investigate leaks. [redacted] suggests that the intelligence community might staff the unit and support the unit with a line-item appropriations. This unit would analyze intelligence leaks reported and then "simply" question a few individuals who stood to benefit from each leak, the perception of Federal interest in preventing leaks would be dramatically strengthened. With the availability of such a
25X1 unit, [redacted] suggests that the intelligence community could be more informed as to how major leak investigations could be undertaken due to the manpower and budget of this specialized unit.

Comment: Formulation of such a unit involving numerous members from the intelligence community would only confuse and compound the difficulties in investigating unauthorized disclosure matters. In addition, his approach to conducting investigations would foster inefficiency and ineffectiveness.

25X1 15. Summary: [redacted] discusses other initiatives that must be taken to improve leak investigations, one of which is to loosen the restrictions on interviewing the news media. 25X1 [redacted] does state that although it is not practical to turn every leak case into a First Amendment confrontation, moreover, in serious leak cases, the only way to proceed, 25X1 according to [redacted] is to call a member of 25X1 the news media before a grand jury. [redacted] also suggests in this paragraph that a special prosecutor would be the appropriate vehicle for use in these matters and that by use of a special prosecutor, the investigation would be perceived as an impartial and independent effort rather than 25X1 a political exercise. [redacted] states that there is authority at the present time for the Attorney General to appoint a nonstatutory special counsel (Title 28 U.S.C., Section 591 (c)) when the Attorney General determines that an investigation may result in a political conflict of 25X1 interest. Despite these authorities, [redacted] is suggesting that legislation be presented which would authorize the President of the United States to appoint an independent counsel to investigate leak matters upon the specific recommendation of a senior official, such as the Director of Central Intelligence.

Comment: The FBI interposes an objection regarding the appointment of an independent counsel to coordinate media leak cases of significant importance, as this agency has always carried out its responsibilities regardless of "political conflict of interest" as he suggests. In proposing that the news media be called before a grand jury to testify regarding leak matters could pose a very serious and far more damaging problem than the actual unauthorized disclosure of classified information. In demanding that the news media appear before a grand jury, the public's interest is enhanced and obvious court battles ensue. The news media would then attempt to obtain additional information, as well as to obtain new information, which would be widely published, thus promoting the cause of the news person (media).

25X1 16. Summary: [redacted] in addition to improved investigations of leaks, recommends that two additional legislative initiatives be considered, the first being to seek legislation which would criminalize the unauthorized disclosure of information by Federal employees and others who have authorized access to this information. 25X1 [redacted] does state that such disclosures of classified information are already covered by the espionage laws (Title 18 U.S.C., Section 793), but the Department of Justice has never successfully prosecuted a leaker under these statutes. (The second legislative initiative does not appear).

Comment: The FBI has no objection to the implementation of new statutes which would provide additional criminal penalties or new criminal penalties for unauthorized disclosure of classified information.

25X1 17. Summary: [redacted] suggests that draft legislation (as submitted under TAB B attached to his memorandum, which is an amendment to Title 18 U.S.C., Section 791, would make it unlawful for a Government employee or contractor, or any person with authorized access to classified information, to willfully communicate such information to a person who is neither a Government employee nor a person with authorized access to such information. This draft legislation would also criminalize disclosures made within five years of an employee terminating his employment with the Government.

25X1 Comment: The FBI interposes no objection to [redacted] proposal.

18. Summary: This paragraph relates to the second and related legislative initiative which allows for injunctive relief when an individual has engaged or is about to engage in unauthorized disclosure of classified information with this legislation and subsequent injunctive relief similar to language contained in the Atomic Energy Act.

Comment: The FBI interposes no objection to this suggestion 25X1 by [redacted]

25X1 19. Summary: [redacted] describes in this paragraph that there are many other steps that can be proposed, some of which have practical limitations on implementation. The first constraint is cost and the second is that security cannot be made so tight that necessary dissemination or use of intelligence 25X1 is inhibited. [redacted] describes a tradeoff in the clearance process between speed and efficiency on one hand, and care and thoroughness on the other.

Comment: No comment.

25X1 20. Summary: [redacted] describes a second constraint regarding the additional steps in addressing unauthorized disclosure
25X1 of classified information, and it is one in which [redacted] states little attention is paid to, and that is public
25X1 opinion. [redacted] explains at length that the public should be made aware of the sensitivity of sensitive intelligence information and that unauthorized disclosure of information of this type can jeopardize the security, safety, and development of sources within the intelligence community.

Comment: This appears to be a general statement in which the FBI has no comment.

25X1 21. Summary: [redacted] in this paragraph is reiterating that the intelligence community embark upon a public program of
25X1 security education, and [redacted] is of the opinion that this public awareness will lead to the leakers' being outcast and not being considered vaguely heroic figures.

25X1 Comment: This is [redacted] conclusion.

25X1

The [redacted] Chairman, Security Committee, Director of Central Intelligence memorandum to the Director, Intelligence Community Staff dated March 29, 1984, on Intelligence Leaks deals with the problems associated with handling leaks. In brief, the memorandum indicates that there should be more public awareness to the problem of leaks, increased education of workers to the severity of leaks and that new legislation be inacted to deal specifically with the disclosure of classified information by cleared individuals to unauthorized persons.

The memorandum indicates that the fragmented, agency-by-agency approach to investigating leaks of information that is disseminated government-wide does not provide a uniform effort. In order to ensure that competent investigative resources are concentrated on areas most likely to yield results, an overall, coordinated effort by a single agency is required. The FBI is the only agency capable of doing this job.

25X1 [redacted] United States Navy, Director, Intelligence Community Staff memorandum to Director of Central Intelligence entitled "Unauthorized Disclosures of Classified Information" undated and classified "Secret" concerns the proposals to counter the unauthorized disclosures of classified information.

Senior members of the Intelligence Community Staff met and recommended five basic categories to counter the unauthorized disclosures of classified intelligence which are increasing in number and severity. The categories are education, legislation, investigations, media interface and information control. With regard to leak investigations, the memorandum stated that the abysmal track record of leak investigations to date dictates that the FBI is the only agency with any chance of success.

SECRET

Miss Mary Lawton for
The Attorney General

The Director of Central Intelligence

Washington, D.C. 20505

Intelligence Community Staff

DCI/ICS-84-7660
20 April 1984

MEMORANDUM FOR: Senior Interagency Group (Intelligence)

25X1 FROM: [redacted]
Executive Secretary

SUBJECT: Meeting - 27 April 1984

1. The SIG(I) will meet on Friday, 27 April at 1000 hours in the
25X1 [redacted] (Room 6W02). The meeting will be chaired by the Director of Central Intelligence; attendance will be principals plus one.

2. The following items will be addressed:

-- Hostile Intelligence Threat Assessment (Recommendations). (Paper for your use at this meeting was distributed on 11 April 1984.)

-- Initiatives to Combat Unauthorized Disclosures of Classified Intelligence Information. (Paper for your use at the meeting is attached.)

25X1 3. Please confirm your attendance by contacting [redacted]
25X1 [redacted] by noon, 26 April.

25X1 [redacted]
for

Attachment:
DCI/ICS 84-3007

Distribution:
Assistant to the President for National
Security Affairs
Attorney General
Deputy Secretary of State
Deputy Secretary of Defense
Chairman, Joint Chiefs of Staff

RECEIVED
APR 24 9 12 AM '84
OFFICE
DEPT. OF JUSTICE

25X1 [redacted]

SECRET

DCI/ICS 84-3007
6 April 1984

MEMORANDUM FOR: Director of Central Intelligence

FROM: Eloise R. Page
Deputy Director, Intelligence Community Staff

SUBJECT: Initiatives to Combat Unauthorized Disclosures of Classified Intelligence Information

1. On 30 March 1984 I convened a meeting in response to your charge to develop administrative, security and legal initiatives which could be taken to help deal with the problem of unauthorized disclosures. At this meeting, which was attended by the Executive Director, the General Counsel, the Director of Security, the Deputy Director of Legislative Liaison, the Chairman of the Security Committee and senior General Counsel representatives, including the Chairman of SECOM's Unauthorized Disclosures Investigations Subcommittee, the papers at Tab A were presented. After some discussion, it was decided that the following proposals should be submitted for your consideration.

I. INVESTIGATION

Nothing is more necessary at this point than to break the cycle of futility by finding an appropriate leak case, having it thoroughly investigated and having the leaker identified and appropriately disciplined.

A. Presidential Statement

-- Congressional and media focus on certain aspects of NSDD-84 diverted attention away from the problem of intelligence leaks and, if anything, the problem has gotten worse. More recently there has been some Congressional recognition of the seriousness of such leaks and we again need to signal Executive Branch concern.

25X1

DOWNGRADE TO UNCLASSIFIED
WHEN SEPARATED FROM TAB A

*We recommend a forceful Presidential statement to his Cabinet and senior White House officials, decrying the harmful effects of leaks. Expressions of Congressional support from the intelligence oversight committees would help immeasurably.

B. Use of a Special Prosecutor

-- Current investigative timidity may derive from the recognition that there are political costs in pursuing an aggressive investigation of media leaks.

*We recommend Attorney General appointment of a special prosecutor (independent counsel) to pursue sensitive leak investigations. The special prosecutor should have all necessary powers, including the ability to bring witnesses before a grand jury.

-- Use of a special prosecutor in appropriate cases will help assure the public, and particularly the media, that the investigation will be impartial and objective and neither politically motivated nor politically constrained.

C. Creation of a Separate FBI Leak Investigation Unit

-- Although we report a significant number of leaks to Justice each year, very few are investigated because Justice is not sanguine about solving such cases and prefers to use FBI resources on other types of cases.

*We recommend creation of a special unit within the FBI to do nothing but investigate intelligence leaks. The Intelligence Community should support a line-item appropriation to finance this unit.

-- Bureau assistance is necessary because certain key government components have no investigative staffs and in other departments and

agencies responsibility and authority are solely internal, with one agency unable to investigate what happened to its information when disseminated to a second agency.

-- Intelligence Community security organizations and the DCI Security Committee must provide appropriate assistance and work closely with this FBI unit.

II. REGULATION OF GOVERNMENTAL CONTACT WITH THE MEDIA

-- Contact between government officials and the press very often is salutary, contributing to public knowledge and informing public debate. Government officials, however, have no license to jeopardize intelligence sources and methods or mishandle classified information. Nevertheless, newsmen regularly brag that they have daily access to some of our most sensitive intelligence publications.

*We recommend:

a) Centralizing within each agency the regulation of all press contacts so a single official is aware of all authorized contacts;

b) Elimination of press building passes giving unsupervised or unrestricted access to government buildings;

c) Requiring employees to record all press contacts relating to their official positions and duties; and

d) Establishment of guidelines for backgrounders and indoctrination of employees on press tactics and proper responses.

III. SECURITY EDUCATION

The public generally regards intelligence leaks as interesting, even titilating and perhaps useful in exposing governmental excess but basically harmless. Leakers are seen as vaguely heroic figures akin to whistleblowers, and leaks are viewed as a kind of game in which the government tries to

hide information while the media trys to find the secrets. Until the public understands that compromises of intelligence sources and methods erode our ability to obtain vital intelligence and hurt the national security more than they contribute to public debate, public support for needed security measures will be lukewarm at best.

A. Presidential Commission

*We recommend creation of a Presidential Commission to review intelligence leaks, to examine steps which can be taken to protect intelligence sources and methods from unauthorized disclosure, to review existing investigative and legal constraints and to make recommendations to improve the situation.

-- Intelligence leaks have been a problem in both Democratic and Republican administrations. A nonpartisan blue ribbon panel could help to generate greater public understanding of the problem and support for appropriate remedial steps.

B. Security Briefings

*We recommend a redoubling of efforts to reach policy level officials in the State and Defense Departments, the National Security Council, and on the staff of the intelligence oversight committees. These security briefings should not be in a lecture format in which the official being briefed listens passively to a recitation of rules. Instead, the briefing must focus on the specific audience, citing the actual damage caused by leaks and explaining how, with a modicum of care, intelligence sources and methods could have been protected with minimum impact on the underlying news story or policy issue. There must be practical guidelines for senior officials on how intelligence material must be safeguarded in dealing with the press.

C. Outreach Program

*We recommend an effort to increase public awareness of the fragility of intelligence sources and methods and the national security implications of intelligence leaks. Senior intelligence officials and public affairs officers should take the time to develop this issue in speeches, articles and other programs which will reach important segments of the public.

IV. LEGISLATION

Arguably, unauthorized disclosures of classified information are in violation of the espionage laws but Justice has never successfully prosecuted a leaker under these statutes. In part, this may be because it is necessary to prove that the individual transmitting the national defense information did so with reason to believe it would be used to the injury of the United States or to the advantage of a foreign nation and in part, because of a reluctance to treat leakers as spies.

A. Criminalizing Leaks

*We recommend new legislation (Tab B) criminalizing the willful unauthorized disclosure of classified information by government employees or other persons with authorized access to classified information.

-- Such legislation would be free of the intent requirements in the current espionage laws and would make willful unauthorized disclosure of classified information illegal per se.

B. Injunctive Relief

-- At the appropriate time after passage of legislation criminalizing the unauthorized disclosure of classified information, we might consider seeking legislation (Tab C) providing for injunctive relief in leak cases similar to that available under the Atomic Energy Act.

2. To the extent appropriate, implementation of these recommendations should be discussed with our oversight committees. In this manner, we can capitalize on the growing Congressional concern about damage to intelligence from leaks and can avoid triggering a partisan political response to actions which seek to deal with a very serious and very urgent problem facing the Community.

25X1

Eloise R. Page

Attachments: As stated.

25X1

MEMORANDUM FOR: General Counsel

25X1 FROM: [redacted]
Associate General Counsel/Chairman,
Unauthorized Disclosures Investigation
Subcommittee, SECOM

SUBJECT: Intelligence Leaks

25X1

25X1

1. Unauthorized disclosures have become so commonplace, investigative action has been so timid, success in solving leak cases has been so infrequent, punishment of the few leakers actually found has been so mild and so hidden and prosecution of leakers has become so improbable that leaking has emerged as a virtually risk-free activity. Indeed, a recent expression of presidential concern about leaks was greeted not by a renewed national resolve to protect fragile intelligence sources and methods, but instead by the concern that security might actually be tightened and that leakers might actually be inhibited. Leakers were turned into heroes and security officials into villains. Leakers have been emboldened and security officials intimidated.

2. It really is time to turn this around by a more vigorous program of security awareness within the Government, and by educating the public at large about the pernicious nature of disclosures which do great damage to our intelligence sources and to the continued availability of vitally needed information while contributing only minimally to public debate. We must pursue leak investigations more vigorously. We must remove those who violate their trust from Government service in a very public and visible way and deal even more harshly with senior officials who should know better and who should set a responsible example for the rest of the bureaucracy. Finally, we need better laws. We need a mechanism to make leak investigations a bipartisan undertaking and we need to stop confusing leakers with either whistleblowers or spies. We must have a law, separate from the espionage statutes, which criminalizes the unauthorized disclosure of classified information by Government employees. But most of all we must reject the conventional wisdom that nothing can be done and eschew those who, as a result of frustration, counsel inactivity and urge us to accept and be resigned to the current deplorable state of affairs.

25X1

TAB A

25X1

3. Security is not an exact science and even the best system occasionally will fail. Nevertheless, the CIA has put together what must be regarded as a model system. Security processing of applicants is rigorous and security indoctrination begins from the moment the employee comes on board. A loyalty to the Agency and an esprit de corps is fostered and a value system geared to protecting intelligence sources and methods is inculcated by security education and security awareness programs. Media contacts are centralized and controlled. The probationary and reinvestigation polygraph programs serve not only to deter unauthorized disclosures, but also to catch the few who become sloppy or who don't care. Leaks are investigated. Security breaches yield predictable punishment and potential leakers know that their jobs will be forfeited.

4. The problem is that CIA and the other intelligence agencies are in the business of disseminating intelligence but the same security controls as exist, for example, at CIA and NSA, do not exist in the consumer agencies. We have, therefore, a security edifice which is very much like a bank with a door of steel 12 feet thick in front but with a rickety screen door in back and until we can insist on the same standards on both the producer and consumer side of the business we will find it very hard to reassure our depositors.

5. There is no single solution, no panacea but there are a number of steps which can be taken. To some extent we must get back to basics and practice the fundamentals. For example, we must more carefully scrub our finished intelligence so that intelligence sources and methods are better protected. We must periodically prune dissemination lists and stop confusing "nice to know" with "need to know." We should make consumers justify their need for continued access to particular publications. We should have more flexible publication formats so that those who need to know about Denmark don't routinely receive reporting on Iran. We should increase our "read and return" programs. We should have exit search programs in Government buildings where classified information is present so people cannot casually walk out with a briefcase full of classified documents, or build up a cache of documents at home.

6. To some extent we need to change the way we routinely do business and to develop new approaches. For example, it simply is not a good idea to give newsmen building passes which enable them to wander at will through Government offices.

7. We should be moving now to try to build into computer-assisted dissemination systems, the kind of security modules which will provide a record as to which document was disseminated to which person, and also to indicate when a hard copy is printed out. Indeed, the computer can generate a unique number for each document which is printed.

8. We need to focus on the growing use of personal microcomputers since this technology can mean that individuals can put highly classified data into the memory of extremely small and highly-portable personal computers. At a minimum, sources and methods information should be protected against being incorporated into such personal computers.

9. We need to cut down the practice of photocopying highly-classified intelligence publications, avoid having them "lying around" and worse yet being passed from desk to desk. As we move more and more into a computerized environment, we can do this by developing for senior policy customers outside the Intelligence Community a "classified executive suite," an attractively furnished room where senior officials can go to read classified intelligence publications. The individual with a key to this "classified executive suite" will log onto a computer terminal and receive his classified mail on the screen. He or she will be able to go to this facility at any convenient time to read the NID or other publications which he is entitled to see. The key to the executive suite will give the consumer the required status and prestige, but the actual reading material can be tailored to his particular needs. The custodian or librarian in the "classified executive suite" can take care of any requests for hard copy and can keep appropriate records as to who received what.

10. When intelligence leaks do occur they must be investigated or at least reviewed. At present this is not done in a systematic way. More needs to be done to evaluate leaks, to prepare damage assessments and to conduct post mortem reviews of the investigation and of the damage after a sufficient passage of time has occurred. Investigations conducted by the various agencies often are inadequate because in many cases responsibility and authority stops at the water's edge and one agency cannot easily investigate what happened to its information when disseminated to a second agency. Thus, it is necessary for the Department of Justice and the FBI to rigorously investigate the unauthorized disclosure of classified intelligence information especially when intelligence sources and methods are involved.

11. The problem is that very few of the leaks reported to Justice by CIA are investigated. We routinely receive as a response to our leak report a form letter which states: "In view of the acknowledged level of dissemination of the information, we are reluctant to direct the FBI to investigate this matter unless you are in a position to identify likely suspects or suspect organizational components. Accordingly, we are unwilling to commence an inquiry until such time as you can narrow the list of potential subjects."

12. The notion that the FBI will not investigate until we identify the suspects is incredible. It is akin to the police saying that they will not investigate a bank robbery at 42nd Street and Fifth Avenue because too many people were in the area but if the bank identifies likely suspects, then the police will investigate. Not only is this bad policy, it proceeds from a false factual predicate. Not all recipients of classified information are equally probable suspects. In most cases, the more junior officers are not credible suspects. In most cases, individuals involved with the intelligence program have equities which are damaged by the unauthorized disclosure and they would have no incentive to leak. Thus, a simple examination of who stands to benefit from the leak can help to focus an FBI investigation. Unhappily, even when our Office of Security has lead information, we rarely find Justice interested in pursuing the matter. Indeed, the decision not to investigate unless the number of persons exposed to the material is very small means, in effect, that leaks from the NID and other similar intelligence publications simply will not be investigated.

13. The reason for this apparent reluctance to investigate leaks derives from the perceived payoffs or lack thereof. The Department of Justice has clearly stated that it regards the chances of solving a leak case as poor and it preferred to husband scarce FBI resources for espionage rather than leak investigations. Justice openly stated that before a newsman could be interviewed by the Bureau, the Attorney General himself needed to give permission and that such permission was not likely to be forthcoming. In sum, it is fair to say that Justice and the Bureau do not see much glory or career enhancing statistics emerging from leak investigations and they act accordingly.

25X1

14. One solution would be to create a special unit within the FBI to do nothing but investigate leaks. The Intelligence Community might detail experienced security officers to help staff the unit and support a line-item appropriation to finance the unit. If the unit would analyze

the intelligence leaks reported to it and then simply question a few individuals who stood to benefit from each leak, the perception of federal interest in preventing leaks would be dramatically strengthened. In addition to this limited effort, major components of the Intelligence Community could be informed as to how many major leak investigations could be undertaken in view of the unit's manpower and budget. If the DCI, for example, knew that the unit could handle ten major CIA leak investigations in the current fiscal year, Agency recommendations could be made to Justice as to which leaks the DCI wanted the unit to focus upon.

15. A number of other initiatives need to be taken to improve leak investigations. One step is to loosen the restrictions on interviewing the press. Although it is not practical to turn every leak case into a First Amendment confrontation, FBI interviews should be a far more routine practice. Moreover, in an appropriately serious case, the only way to proceed may be to call a member of the press before a grand jury. It is recognized that there could be a political cost in doing this but that could be dissipated by use of a special prosecutor so that the leak investigation is not perceived as a political exercise but rather as an impartial and independent effort to stop the hemorrhaging of national security information. There is now authority for the Attorney General to appoint a non-statutory special counsel and there is authority (28 U.S.C. § 591(c)) for the Attorney General to petition the court for appointment of a special counsel when he determines that an investigation may result in a political conflict of interest. Despite these authorities, consideration should be given to recommending separate legislation to specifically authorize the President to appoint an independent counsel to investigate leaks upon the recommendation of a senior official such as the DCI. A draft bill is included at Tab A.

16. In addition to improved investigations of leaks, two additional legislative initiatives should be considered. The first is to seek legislation which would criminalize the unauthorized disclosure of information by federal employees and others who have authorized access to classified information. Arguably, such disclosures of classified information already are covered by the espionage laws, (i.e., 18 U.S.C. § 793) but Justice has never successfully prosecuted a leaker under these statutes. In part, this may be because it is necessary to prove that the individual transmitting the national defense information did so with reason to believe it would be used to the injury of the United States or to the advantage of a foreign nation, and in part because of a reluctance to treat leakers as spies.

17. The draft legislation at Tab B would eliminate the intent requirement and make it unlawful for a Government employee or contractor or any person with authorized access to classified information to willfully communicate such information to a person who is neither a Government employee nor a person with authorized access to such information. In order to ensure that an individual does not evade the law by making such disclosure after leaving the Government or after the termination of authorized access, the draft legislation also would criminalize such disclosures made within five years after leaving the Government or losing access. This legislation (without the five year after-service provision) was drafted by Gary Chase and George Clarke in 1982, and it was coordinated with the Justice Department and cleared by the Administration for transmittal to the Congress, but it never actually was sent to the Hill.

18. The second and related legislative initiative is to seek legislation allowing for injunctive relief when an individual has engaged or is about to engage in any acts which would violate the proposed law prohibiting unauthorized disclosures of classified information. (Tab C) At present, similar language is contained in the Atomic Energy Act.

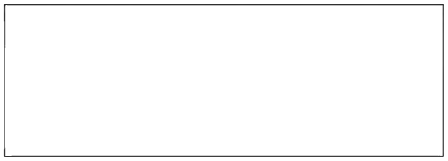
19. There are many other steps which can be proposed but there are practical limitations on the implementation of additional security controls, the imposition of more effective administrative procedures, the resort to more powerful investigative techniques or the development of new legal remedies. The first constraint is cost. It is well understood that security cannot be made so tight that necessary dissemination or use of intelligence is inhibited. There is a tradeoff, for example, in the clearance process between speed and efficiency on the one hand and care and thoroughness on the other. We all know that security has a price tag and we regularly engage in a cost-benefit analysis in an effort to achieve a proper balance.

20. The second, and perhaps more important constraint, is public opinion, but we rarely pay sufficient attention to this factor. Nevertheless the public mood sets the limits as to what is tolerable and acceptable. Requiring persons who have had access to sensitive intelligence information to submit writings on intelligence for prepublication review is regarded within the Intelligence Community as a sensible measure to ensure against the inadvertent disclosure of classified information. Media and congressional judgments on this procedure have been quite different and quite negative.

Even though the intelligence agencies can do nothing more than advise the author as to the existence of classified information, and must go to court in order to enjoin publication of classified information, prepublication review is labeled "life-time censorship" stifling public debate and the free flow of ideas. On the other hand, a far more intrusive practice, the search, without a shred of probable cause, of all passengers and their luggage at airports, although initially controversial, now excites little opposition or criticism. In the one case, the security measure is poorly understood and the need for it even less understood. In the second case, the overriding concern for personal safety makes a far more draconian security measure totally acceptable. The public must come to realize that disclosure of legitimately classified information -- and there should be no other kind -- poses a clear and present danger to their security and their safety in an ever more dangerous world. They must come to realize that intelligence sources can easily dry up, that expensive technical systems can become subject to countermeasures and intelligence relationships painfully built up can quickly be lost. Depriving policy makers in the defense and foreign policy arenas of information needed to make rational choices among policy alternatives, harms each and every one of us, hurts us in our pocketbooks, and erodes the quality of life for American citizens.

21. The current rather casual public attitude toward leaks has not sufficiently been challenged and a climate of opinion conducive to leaks has been allowed to develop virtually unchecked. It is extremely important, therefore, that the Intelligence Community embark upon a public program of security education. It is only when the reasons for our profound concern about intelligence leaks are understood that we will be able to count on public support for protecting our vital intelligence sources and methods. Only then will leakers be outcasts and not vaguely heroic figures.

25X1



OFFICIAL USE ONLY

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM D-069

29 March 1984

MEMORANDUM FOR: Director, Intelligence Community Staff

25X1 FROM: [redacted]
Chairman

SUBJECT: Intelligence Leaks

25X1 REFERENCE: DCI MEMO, [redacted] dated 23 March 1984, Subject: Intelligence Leaks and Counterterrorism Capabilities

1. The referent memorandum and the recent SSCI hearings have raised new hopes that something can be done at last about those who breach their oaths and reveal classified intelligence to the news media. The following observations on the leak situation may be useful to you in carrying out the DCI's charge.

2. While Senator Biden's helpful attitude is gratifying, there is a need to stimulate public opinion against leaks of classified information. There is a great groundswell of apathy about leaks, both within the government and among the general public. It is essential that new leak legislation, if it can be passed, not be regarded with the same enthusiasm as the Volstead Act.

3. There has been little opportunity to take the anti-leak message to rank-and-file government employees. Even worse, the public receives all its information about leaks and anti-leak efforts from the news media. While the DCI videotape has been shown to high-level audiences in some, not all, Intelligence Community agencies, it has not been generally presented to middle and lower graded personnel, even in CIA.

4. We are not doing enough to create a climate of acceptance for anti-leak efforts. Almost without exception, audiences viewing the DCI leak videotape have expressed the belief that no progress will be made until senior officials of the government stop leaking classified information for their own purposes. The opinion persists that the public chastisement of one or more identified high level leakers is essential to marshalling any anti-leak support. The message is clear--mere words are not enough. The government must demonstrate that leaks are a sufficiently severe problem to warrant decisive, well-publicized action against senior, well-connected officials.

5. There is a reasonable reluctance to use the Espionage Act to prosecute leakers. Legislation is needed to deal specifically with the disclosure of classified information by cleared individuals to unauthorized persons. No matter how one views it, this is a different crime from espionage. Nevertheless, it is no less a breach of trust by a federal official than illegal use of a limousine, disclosure of crop futures, or misappropriation of federal funds. It deserves its own law. We should not drive tacks with a sledge hammer. We have offered, then withdrawn, legislative proposals on this topic for the past two years.

6. As the leak situation grows worse, our posture to combat leaks also seems to be going downhill. The Brooks Bill, if passed, would hamper the anti-leak effort. More important, it would send a message that efforts to combat leaks are somehow immoral, unconstitutional,or worse. It is essential that Congressional liaison officers throughout the Community do everything possible to educate members of both Houses on the pernicious nature of leaks and the extremely disadvantaged posture of the government in combatting them. A solid defeat for the Brooks Bill is an indispensable step in our effort to turn public opinion around.

7. CIA and the rest of the Community need to determine as precisely as possible what the leak story is and how much of that story can be told publicly; how much more can be told to Congressional leaders, and how much can be told to top Administration officials. Unless we can present a credible story that the US intelligence effort is being significantly damaged by leaks, no amount of hand wringing is likely to have any effect, whatsoever.

8. We need to determine ways to get the general story before the public and the specifics to those who can help lead the way back from apathy. Having a good story doesn't help unless we can get people to listen. The DCI anti-leak videotape has been an excellent counsciousness-raising exercise, but there has been a constant uphill struggle to get audiences to view it. We need to produce a new, hard-hitting, factual message on leaks and obtain authority to require cleared personnel throughout the government to attend.

9. The fact that after four decades, the DCI still finds the slogan "loose lips sink ships" useful indicates that posters are a powerful medium. We should mount a poster campaign against leaks throughout the government. Posters provide the message to masses of people without requiring any action on their part.

10. As has been reiterated, the current procedures for investigation of unauthorized disclosures are geared to failure. The fragmented, agency-by-agency approach to investigating leaks of information that is disseminated government-wide doesn't provide a uniform effort. In order to ensure that competent investigative resources are concentrated on areas most likely to yield results, an overall, coordinated effort by a single agency is required. The FBI is the only agency capable of doing the job. It is also essential to the continued protection of intelligence sources and methods that the investigation be closely coordinated with senior Intelligence Community

officials who can determine the risk of additional revelations of classified information at every step of the investigation and recommend appropriate action to avoid compounding our problems.

11. The fragmented approach to investigation does not permit any analysis of leaks for possible patterns. Centralized investigation and coordination would afford the opportunity to analyze the content, apparent intent, possible sourcing, etc., in order to focus investigative efforts where they are likely to yield results. Sophisticated investigative and analytical techniques, as currently being applied to the fight against narcotics, need to be used against leaks. The current simplistic approach does not work.

12. To avoid having an anti-leak effort evaporate in a cloud of frustration, there should be personnel and other resources dedicated to the investigation and prosecution of leaks, preferably with a Congressional mandate. The current unsophisticated, relatively low level, effort appears to result from reluctance to devote resources to a no-win situation. If the resources and appropriate guidelines can be made available, we can win, at least some of the time. A concerted effort to mount a strong pilot operation offers the best chance of success.

13. Senator Biden's concern about lack of utilization of "graymail" procedures illustrates two points that must not be ignored. The first is that the passage of legislation, per se, is not enough to cure a bad situation. The second is that nothing can be done about the leak problem unless some of the offenders are identified and penalized.

14. I have telephoned all the members of the Security Committee and requested their thoughts on new approaches to the leak problems. Their responses will be provided to you when received.

15. Finally, I propose that we consider recommending appointment of a presidential commission on unauthorized disclosure of classified information. A bi-partisan group of distinguished present and former members of all three branches of government could be given all the facts and asked to report and recommend remedial action. Coming from such a broad-based group, the recommendations should command widespread support and would provide a means of informing the American people of the gravity of the threat, if not the details of it. Formation of a commission would provide a way to meet several of the needs enumerated above. The primary drawback is that this is an election year. Although timing is important, the action could be taken after the election, because the problem will still be with us.

25X1

SECRET

Director
Intelligence Community Staff
Washington, D.C. 20505

ICS-0802-83

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

25X1 FROM: [redacted]
Director, Intelligence Community Staff

25X1 SUBJECT: Unauthorized Disclosures of Classified Information [redacted]

1. Senior members of the Intelligence Community Staff have met to consider responses to your call for proposals to counter the unauthorized disclosures of classified intelligence which are increasing in number and severity. The recommendations of the group are in five basic categories -- education, legislation, investigations, media interface and information control. This memorandum discusses proposals in each of these categories.

2. Education - There appears to be a lack of appreciation of the consequences of the unauthorized revelation of classified intelligence information, both to the national security and to the individual making the disclosure. Each recipient of Sensitive Compartmented Information (SCI) is indoctrinated on the potential damage to the national security of such revelations, as well as the penalties prescribed in Title 18, Sections 793 through 798. Nevertheless, incidents continue which indicate that these elements of risk are not being taken seriously. Recipients of classified intelligence must be convinced that its unlawful revelation is reprehensible, and that individuals who take it upon themselves to decide when the system may be ignored place the national security and themselves in jeopardy.

3. In wartime, the population recognizes the need to keep military secrets. The concept that "loose lips sink ships" is well accepted. We need a campaign, beginning with the President, to convince all concerned that classified information must be protected if we are to avoid national disaster. A vigorous Presidential charge to the Cabinet and the Executive Office of the President, relayed through channels to all levels, is an essential element of this campaign.

4. Awareness of the importance of security to intelligence must be extended to the Congress. The whole-hearted cooperation of both legislators and staff members is indispensable. Not only is Legislative Branch support needed to safeguard the material provided to the Congress, but also to put teeth into the anti-leak effort.

ILLEGIB

5. To make this effort credible, documents must be classified properly and concern about disclosures should be limited to those affecting national security.

6. A one-time effort to sensitize the government and the public to the disastrous consequences of illegal disclosures, even one kicked off by the President, has a limited half-life. There must be a planned follow-up. In addition to the obvious reindoctrination efforts, consideration should be given to an ongoing program of damage-oriented "lessons learned" presentations. These are envisioned as timely, specific, succinct and technically competent videotape shows detailing the nature of the unauthorized disclosure and the specific losses suffered as a result. They would be shown to audiences cleared for the compromised information as a means of reinforcing the need for strong security.

7. Because of the general derision with which the media regard government efforts to stop leaks and because the generic term "leak" is associated with disclosures that are politically embarrassing, It may be advisable to avoid that term and speak only of "unauthorized disclosures of classified information."

8. Legislation - The existing espionage laws were drafted to protect U.S. secrets from foreign agents. They did not contemplate the hemorrhaging of classified data that has followed the media explosion. The divulgence of classified information to the Russians by way of Jack Anderson's column, for example, is a relatively new phenomenon. Even though the intentions of the leaker may be to nobly inform the public of facts he thinks should be known, the results are the same as directly transmitting the information to the KGB.

9. Attached is a copy of the proposed bill to prohibit certain unauthorized disclosures of classified information. Formulated on the basis of the Willard Report, it is an excellent vehicle for closing the loophole that allows individuals to ignore classifications and make their own decisions about what must or must not be kept secret. Passage of such a bill would make it clear that both the legislative and executive branches are serious about preserving our ability to keep our national security secrets. It would then remain for the judiciary to show the same resolve.

10. The chances of passing the unauthorized disclosures bill are directly related to the Congress's perception of how responsibly the Executive Branch uses its classification powers. As noted above, the effort to educate government employees (and the public, to the extent possible) on the need for effective secrecy must also include the Congress and legislative staff personnel. The means of reaching this objective are the same for both branches of government -- graphic demonstrations that unauthorized disclosures are costly in terms of money, national defense, intelligence capabilities, and sometimes, human lives.

11. Legislation also is needed to make the unauthorized possession of classified material a crime. It is illogical for the U.S. Government to be

unable to bring charges against, or at least sue to recover classified material from, Jack Anderson, who makes a mockery of classification, or from Aviation Week and Space Technology, which has printed classified satellite imagery. If the U.S. would take action against an ordinary citizen, it should act with the same vigor against journalists who damage the national security. The Attorney General and the General Counsels of the Intelligence Community should begin a crash program to draft a legislative proposal and to review the possibilities of action even without a new law.

12. Whether or not the effort to pass new legislation is successful, it is vital that Congress be included in any awareness-raising program. A secondary objective would be to raise the security standards of the congressional staffs. Many staffers have access to more sensitive information than some CIA or NSA personnel, who are polygraphed as well as backgrounded, and are subject to periodic reprocessing. Congressional staffers are not steeped in the discipline of security as are the intelligence professionals, and would almost certainly benefit from a greater appreciation for the need for secrecy.

13. Finally, the problem of reinforcing the responsibilities of formerly cleared recipients of classified information to continue to maintain secrecy requires attention. A periodic reminder by mail might be considered, but except for CIA and NSA, it could be difficult to identify those who should receive them. In the future, the archival file of the Community-wide, Computer-assisted Compartmented Control (4C) System, which will contain the identities of individuals formerly approved for access to SCI, should assist with this problem. Meanwhile, the message needs to be spread that our "old boys" can do a lot of harm by talking too much. Cleared persons still employed in government must be reminded frequently and forcefully that those who have retired, or taken jobs in the industrial sector, may not legally receive classified information unless they are specifically cleared for it.

14. Investigations - The investigation of unauthorized disclosures has rarely proven successful over the years. The broad dissemination required of intelligence reporting, the lack of an effectual investigative program throughout the government, an apparent tolerant attitude toward those who make illicit disclosures, and the absence of a legislative basis for action have made for a highly frustrating situation. NSDD-84 offers hope for greater success in the future, but there is much to be done.

15. Although leak investigations are searches for needles in haystacks, occasionally good investigative work will produce results. Unfortunately, unauthorized disclosures to the media are consensual acts between two parties, neither of whom is likely to admit participation, and one of whom enjoys a special degree of privilege under the First Amendment. Legislation will help, but there can't be a trial until a defendant is identified. The abysmal track record of leak investigations to date dictates that the Federal Bureau of Investigation is the only agency with any chance of success. Fragmented, single-agency efforts simply do not work. Nor does the proposal to form interagency units to investigate unauthorized disclosures offer any reasonable hope for improvement.

16. Even the FBI will require some help -- the full cooperation of other agencies, the legislation discussed earlier, and guidelines that permit the use of as full a range of investigative tools as possible. The Attorney General and the Director of the FBI should be instructed by the President to provide the most permissive guidelines possible, consistent with the protection of civil liberties, for FBI investigations of unauthorized disclosures of classified information. In addition, appropriate manpower allocations to the FBI should be made to ensure a vigorous effort to solve unauthorized disclosures. Without this, the Bureau cannot be expected to neglect other important investigations to undertake tasks that offer a low probability of success and almost certain criticism in the press.

17. Because of the nature of unauthorized disclosures, the likelihood of developing conclusive evidence is low. In fact, the investigative tool most likely to succeed is the polygraph, if conventional investigation can narrow the number of suspects sufficiently to employ it. If a suspect confesses as a result of polygraph interview the case is solved. If, however, in the face of clear-cut polygraphic evidence of deception he continues to deny culpability, the problem of acceptability of polygraph evidence arises.

18. While prosecution on the basis of polygraph charts is extremely unlikely to succeed, the government could revoke the individual's clearances or access approvals on that basis. This would effectively neutralize future disclosures by that individual, but could result in a lawsuit to regain the approvals. The Justice Department and Intelligence Community legal counsels should be tasked to research the grounds upon which such a suit could be defended and the likelihood of success.

19. Action based primarily upon polygraph results is certain to bring strong media criticism. The polygraph process is little understood and the press has fostered this misunderstanding by pressing the theme that the instrument itself is unreliable. Consideration should be given to preparing an educational program to be used first with senior officials of the Executive Branch and with legislators. It should demonstrate that the effectiveness of the process doesn't depend totally upon the machine, but is a technique to aid a skilled interrogator. If a convincing effort can be mounted, it could be brought to the public and even to the news media. If the Intelligence Community can't provide objective, rational evidence that the polygraph process is reliable, the entire effort to combat unauthorized disclosures may be in serious trouble.

20. Press Interface - NSDD-84 mandates policies to govern contacts between media representatives and agency personnel, leaving implementation to the individual agencies. The effort to eradicate unauthorized disclosures would be assisted greatly by the adoption of uniform rules for all agencies.

21. The discussion of government information, especially sensitive intelligence, by a government employee is not a private, personal matter. There seems no reason why the government cannot require the reporting of all contacts with the news media, during or outside of duty hours, in which

government business is discussed. Failure to follow such a rule could be made subject to administrative sanctions of varying severity. Data on such contacts could be computerized, by names of government employees, names of media representatives, subjects of discussions and dates of contacts, providing a means of determining a great deal of information that could take inordinate amounts of investigative effort. It wouldn't tell who made unauthorized disclosures, but it would provide a means of determining who might have had the means and the opportunity, and possibly even the motive to have done so.

22. It would be ideal, from the standpoint of security, to abolish backgrounders. Recognizing that this isn't going to happen, there should be firm control of background briefings to the press. There must be clear-cut guidelines on who may authorize and present backgrounders. Every such briefing should be attended by a security or public affairs officer who knows what is sensitive about the topic being discussed and is capable of offering guidance to the briefer. A record should be kept of briefings by names of participants and authorizing officials, dates and topics, preferably in a computerized mode. Presenters of background briefings should be required to prepare summaries of what was presented. These should be cross-referenced to the automated index of background briefings. The documentation of this information and its retrievability will not only serve as an invaluable investigative resource, but its existence will promote prudence in the presentation of backgrounders and in other dealings with the press.

23. Even if all these proposals were adopted, there would be individuals who would continue to divulge classified information to the press. But they would find themselves operating at considerably greater risk. Simple failure to comply with the reporting requirements would be cause for administrative sanctions, and it would become easier to detect such failures by having a reliable record of compliance. It is likely that associations between government personnel and media representatives are known to at least some associates of both, and the possibility of being reported by a concerned colleague would be enhanced by the revised rules. An effective education program about leaks should have the salutary effect of highlighting to their associates those who may deal with the media without observing the reporting requirements. If those who comply are sufficiently convinced of the need for regulation of press contacts, they may be inclined to "blow the whistle." It would then be necessary for the government to demonstrate the seriousness of its intent by taking administrative action against the nonreporting individuals, regardless of their positions.

24. The matter of "authorized" or "official" leaks needs close attention. If the appropriate official determines it is in the national interest to release for publication information that was classified until that point, there should be a means of recording that fact. Such a record would appropriately be kept somewhere in the Executive Office of the President. This record could provide a means of avoiding the expenditure of resources to investigate such disclosures as "leaks."

25. Finally, the revolving door practice of appointing national media personalities as top level government press officers should be carefully reexamined. Such appointments must face the incumbents with conflicts of interest and severely ambivalent feelings, both during and after their federal service. It may be unrealistic to expect them to deny their colleagues information which they feel is unjustifiably classified and to expect them to forget, and never use, information they received officially.

26. Information Control - Some people believe there are enough information control policies, procedures and regulations on the books to bring the government to a complete halt if they were strictly applied. While this view may have some merit, it should not serve as an excuse for not trying to secure our sensitive information. The concept that security is everybody's business must not be given lip service and then cast aside.

27. Except for the need for developing a strong, national information control program for the emerging electronic information systems, it is unlikely that more document control regulations are needed or practicable. What is needed is for everyone to be educated in the existing policies and procedures and to make a renewed effort to comply. While everyone claims to know the regulations, it is likely that few could pass a comprehensive test on information security and control.

28. Steps to improve information control would include detailed comparison of practices with policies; the reeducation of all personnel in information security, and a motivational program to enhance awareness of the consequences of improper handling of sensitive intelligence. Better information control is needed, but it must come from motivated people. More regulations are not the answer.

29. Summary - Unauthorized public disclosures of classified information in the news media are damaging to the national security. Our defense against them must come from within, from those who are cleared for access to, and who have signed agreements to protect, classified information. It is clear that some of these people, for reasons of their own, have not kept their word. It also appears that neither the overall level of concern about this situation nor the government's capability for remedial action is up to the job.

30. To encourage wholehearted support of our efforts to protect classified information, we must convince those who have agreed to keep the secrets that they have a moral and legal obligation to keep that convenant. The rules on SCI are simple and clear. It is inconceivable that anyone who gives such information to uncleared individuals is unaware of what he is doing. Therefore, such persons must be unconvinced of the seriousness of the security program.

31. A massive reeducation program for all legitimate recipients of classified information is the first step in attempting to achieve the necessary change in attitude.

32. A policy and resource commitment to the solution of at least the most flagrant cases of unauthorized disclosure is also needed. This means the devotion of sufficient FBI assets to investigations and an all-out effort to obtain passage of unauthorized disclosure laws.

33. A severe tightening of policies concerning relationships of cleared individuals with media representatives is essential. To be meaningful, this must include strict guidelines, reporting procedures, information retrieval capabilities, and impartial administrative penalities for noncompliance.

34. Renewed awareness of information control policies and procedures and their importance to the national security is needed. If classified documents can be turned over to the media or other unauthorized persons without being noticed, the system isn't working. It must be made clear that "the system" really is the people who operate it.

35. If you wish elaboration or action on any of the above items, appropriate elements of the Intelligence Community Staff are prepared to assist in any way possible.

25X1

Attachment:
Draft unauthorized disclosures bill

All paragraphs of the text
are classified SECRET

New version of proposed 18 U.S.C. 791 is attached. Note that the cover language specifies that the proposal would have to be recoordinated within the Administration before being sent to the Congress

In the course of Administration development of the Fiscal Year 1984 Intelligence Authorization Bill, the Intelligence Community obtained from the Office of Management and Budget clearance of a proposal to establish criminal penalties for certain unauthorized disclosures of classified information. The proposal was based in part on the report of the Interagency Group on Unauthorized Disclosure of Classified Information chaired by Deputy Assistant Attorney General (Civil Division) Richard K. Willard. It was coordinated with Deputy Assistant Attorney General (Criminal Division) Mark Richard, as well as with the Office of the Secretary of Defense/Legislative Affairs.

For a number of reasons, including the issuance of NSDD-84 just before the Authorization Bill was forwarded to the Congress, and in deference to the intelligence committees' preference for handling the Intelligence Authorization in as unobtrusive a manner as possible, the unauthorized disclosures proposal ultimately was not transmitted as part of the Authorization Bill. The climate for transmittal of the proposal as part of the Fiscal Year 1985 Intelligence Authorization Bill also was considered unfavorable, due to continuing controversy over NSDD-84.

The proposal (attached) has been modified to include former officers or employees for a period of five years following termination of their government service. It has been reconfigured as a separate bill, and prepared for transmission

at an opportune moment as an initiative from the DCI. The proposal would have to be recoordinated within the Administration before being sent to the Congress.

A BILL

To protect against injury to the national defense and foreign relations of the United States by prohibiting certain unauthorized disclosures of classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That Chapter 37 of title 18, United States Code, is amended by adding at the beginning thereof the following new section:

"§ 791. Unauthorized Disclosures

(a) Whoever, being or having within the last five years been an officer or employee of the United States or a person with authorized access to classified information, willfully discloses, or attempts to disclose, any classified information to a person who is not an officer or employee of the United States and who does not have authorized access to it, shall be fined not more than $10,000, or imprisoned not more than three years, or both.

(b) Whoever, being an officer or employee of the United States, willfully discloses any classified information to an officer or employee of the United States with the intent that such officer or employee disclose the information, directly or indirectly, to a person who is not an officer or employee of the United States and who does not have authorized access to it, shall be fined not more than $10,000, or imprisoned not more than three years, or both.

(c) As used in this section--

(i) the term "classified information" means information or material designated and clearly marked or represented, pursuant to the provisions of a statute or Executive order, as requiring protection against unauthorized disclosure for reasons of national security;

(ii) the term "disclose" or "discloses" means to communicate, furnish, deliver, transfer, impart, provide, publish, convey, or otherwise make available;

(iii) the term "authorized access" means having authority, right, or permission to receive information or material within the scope of authorized intelligence activities or pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency who is empowered to classify information, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which governs handling of classified information by the respective House of Congress.

(d) Nothing in this section shall be construed to establish criminal liability for disclosure of classified information in accordance with applicable law to:

(i) any court of the United States, or judge or justice thereof; or

(ii) the Senate or House of Representatives, or any committee, subcommittee or joint committee thereof.".

SEC. 2. The table of contents of Chapter 37 of title 18, United States Code, is amended to include the following caption:

"791. Unauthorized Disclosures".

SECTION BY SECTION EXPLANATION

Section 1 of the Bill amends chapter 37 of title 18, United States Code, to include a section 791 prohibiting certain unauthorized disclosures of classified information. Section 2 of the Bill makes the corresponding changes in the table of contents for chapter 37 of title 18.

Proposed section 791 of title 18, United States Code, provides criminal penalties for willful unauthorized disclosures of classified information by federal employees and others who have authorized access to classified information, such as government contractors. With the narrow exceptions of unauthorized disclosures of atomic energy Restricted Data, communications intelligence/cryptography information, and the identities of covert agents, willful unauthorized disclosures of classified information by those entrusted with it by the government are not per se offenses under existing federal criminal statutes.

Subsection (a) of § 791 prohibits willful disclosure or attempted disclosure of classified information, by a federal civilian or military officer or employee or other person with authorized access to such information, to any person who is neither a federal civilian or military officer or employee nor a person with authorized access to such information. The subsection provides criminal penalties of not more than three years imprisonment or a $10,000 fine, or both, for such willful unauthorized disclosure of classified information.

Subsection (a) of § 791 would prohibit unauthorized disclosures by persons who are, or who have within the last five years been, officers or employees of the United States. It also would apply to persons who have authorized access to classified information or who have had such access witnin the last five years. This limited retroactive feature is important to ensure that criminal liability under proposed section 791 is not evaded by an individual who begins to make unauthorized disclosures shortly after leaving government service or having had authorized access.

Subsection (b) of § 791 prohibits willful disclosure of classified information by a federal civilian or military officer or employee to another such officer or employee with the intent that the latter disclose the information, directly or indirectly such as through a chain of intermediaries, to a person who is neither a federal civilian or military officer or employee nor a person with authorized access to the classified information. The criminal penalties for such an offense are identical to those provided for the offense defined in subsection (a).

Subsection (c) of § 791 defines key terms employed in subsections (a) and (b) in defining the offenses of willful unauthorized disclosure. Paragraph (i) defines "classified information" to consist of information or material designated as requiring protection against unauthorized disclosure for reasons of national security pursuant to a statute or Executive order. Paragraph (ii) defines the term "disclose" or "discloses" to include all forms of disclosure enumerated in the existing provisions of 18 U.S.C. §§ 793-798 and 50 U.S.C. § 426. Paragraph (iii) defines the term "authorized access" to include authority or permission to receive information within the scope of authorized intelligence activities or pursuant to the routine security clearance processes of the Executive branch, orders of the courts of the United States, or rules of either House of Congress. Authorized intelligence activities are those conducted pursuant to statute or Executive order, such as the current Executive Order 12333 governing United States intelligence activities.

Subsection (d) of § 791 assures that no criminal liability will attach under subsections (a) or (b) to otherwise lawful disclosure of classified information to the Congress or the courts.

Honorable Thomas P. O'Neill, Jr.
Speaker of the House of Representatives
Washington, D.C. 20515

Dear Mr. Speaker:

This letter transmits for the consideration of the Congress legislation to provide criminal penalties for the unauthorized disclosure of classified information by individuals who have had authorized access to such information. The legislation is designed to deter unauthorized disclosures of classified information, which damage the national security interests of the United States and raise grave questions about the ability and willingness of the United States Government to protect its secrets.

With the exception of disclosures of information in the narrow categories of atomic energy Restricted Data, communications intelligence or cryptography, and identities of covert agents, disclosures of classified information by government employees and others with authorized access to classified information, such as government contractors, do not constitute per se criminal offenses. In many circumstances such conduct would violate the Espionage Act or statutes protecting government property from theft, but a variety of legal and practical problems usually prevent such prosecutions. The proposed legislation contains straightforward, easily understood, and readily enforceable provisions prohibiting willful unauthorized disclosure of classified information by government employees and others who have had authorized access to classified information.

The proposed legislation has been narrowly tailored to establish criminal sanctions for unauthorized disclosures of classified information only when committed by individuals who, by virtue of their acceptance of employment in positions of trust involving the national security, have freely undertaken the legal and moral obligation to protect classified information. The legislation has also been crafted carefully to preserve access to classified information by the executive, legislative, and judicial branches of government.

Timely consideration of this legislation of great importance to the continued security of the nation would be greatly appreciated. The Office of Management and Budget has advised that enactment of the proposed legislation would be in accord with the President's program.

Sincerely,

William J. Casey
Director of Central Intelligence

Two versions of the

Injunction Provision

TAB C

Version 1
Injunction Against Violation of Proposed § 791

A BILL

To protect against injury to the national security and foreign relations of the United States by preventing certain unauthorized disclosures of classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That Chapter 37 of title 18, United States Code, is amended by adding the following new subsection:

"§ 791a.

Injunction Proceedings

Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts which constitute or will constitute a violation of any provision of section 791 of this title, the Attorney General on behalf of the United States may make application to the appropriate federal district court for an order enjoining such acts, and upon a showing that such person has engaged or is about to engage in any such acts, a permanent or temporary injunction, restraining order, or other order may be granted.".

SEC. 2. The table of contents of Chapter 37 of title 18, United States Code, is amended to include the following caption:

"791a. Injunction Proceedings".

Version 2
Injunction Against Violation of Proposed § 791
and Against Publication of Information Disclosed in Violation
of that Section

A BILL

To protect against injury to the national security and foreign relations of the United States by preventing certain unauthorized disclosures of classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That Chapter 37 of title 18, United States Code, is amended by adding the following new subsection:

"§ 791a.

Injunction Proceedings

Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts which constitute or will constitute a violation of any provision of section 791 of this title, or has published or is about to publish information disclosed in violation of that section, the Attorney General on behalf of the United States may make application to the appropriate federal district court for an order enjoining such acts or publication, and upon a showing that such person has engaged or is about to engage in any such acts, or in the case of publication that such publication would cause grave, immediate, direct and irreparable harm constituting a clear and present danger to the national security or foreign relations of the United States, a permanent or temporary injunction, restraining order, or other order may be granted.".

SEC. 2. The table of contents of Chapter 37 of title 18, United States Code, is amended to include the following caption:

"791a. Injunction Proceedings".